

AUG 30 2007

Attorney's Docket No.: 42P15739

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application for:

Francis X. McKeen

Application No.: 10/644,399

Filed: August 19, 2003

**For: METHOD AND APPRATUS TO
PROVIDE PROTECTION FROM A
BUFFER OVERFLOW ATTACK**

Examiner: Meonske, Tonia L.

Art Group: 2181

Conf. No.: 7924

Mail Stop Amendment
Commissioner for Patents
P. O. 1450
Alexandria, VA 22313-1450

Dear Sir:

I, Francis X. McKeen, hereby declare that:

1. I am a citizen of the United States of America.
2. I currently reside at 10612 NW LeMans Ct. Portland, OR 97229.
3. I am currently an employee of Intel Corporation in Santa Clara, California.
4. I have been an employee of Intel Corporation since Oct 30, 1995.
5. My current title at Intel Corporation is Hardware Engineer.
6. I am the sole-inventor of the above-identified patent application.

7. I have reviewed U.S. Patent 6,996,677 issued to Lee et al. ("Lee"), which was filed on February 20, 2003. Lee claims priority from provisional patent application No. 60/429,839 filed on November 25, 2002. The Examiner cites Lee against the claims of the above-identified application.

8. The invention disclosed and claimed in the above-identified patent application was conceived in the United States of America at least as early as October 18, 2002, as evidenced by Intel Corporation Invention Disclosing Form (IDF) having ID #28002 (a copy of which is attached herein). This document was reduced to writing internally within Intel Corporation at least as early as the date on the document; i.e., October 18, 2002. The foils referenced by the IDF is a presentation entitled "LT Stack Protection," (a copy of which is attached herein). This document demonstrates conception of the claimed invention of the instant application. Although Revision 0.1 of the LT Stack Protection document indicates an August 28, 2007 date, as indicated in the attached screen print, the document was first created on March 9, 2001. Revision 1 of the LT Stack protection document was completed at least as early as the date on the date on the IDF document; i.e., October 18, 2002. Between at least October 2002 and its constructive reduction to practice by the filing of the above-captioned patent application on August 19, 2003, I directed simulations and various testing in a diligent effort to reduce the invention to practice. Therefore, the conception and diligence towards reduction to practice of the invention disclosed and claimed in the above-identified patent application occurred prior to the filing date of Lee.

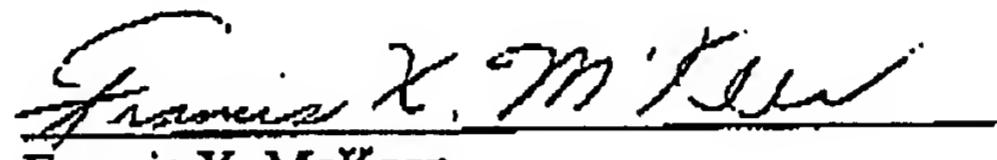
9. The documents provided herewith are confidential. It is Intel Corporation's practice to maintain in secrecy all confidential documents. I believe that the documents have at all times prior to the filing date of the above-captioned application been maintained in a confidential manner.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like are

punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the above-identified application or any patent issued thereon.

Respectfully submitted,

Dated: August 30, 2007



Francis X. McKeen

Full Name:

Francis X. McKeen

Citizenship: United States of America

Residence: 10612 NW LeMans Ct. Portland OR 97229

**RECEIVED
CENTRAL FAX CENTER**

Aug-30-07 02:33pm From-B S T Z
Rev. 16, 5/02

AUG 30 2007

310 820 5988

T-161 P.018/028 F-111

INTEL INVENTION DISCLOSURE
ATTORNEY-CLIENT PRIVILEGED COMMUNICATION
located at <http://legal.intel.com/patent/index.htm>

DATE: October 18, 2002

MOBILE PLATFORMS/MPG/MPA

It is important to provide accurate and detailed information on this form. The information will be used to evaluate your invention for possible filing as a patent application. Invention Disclosure forms MUST be sent electronically via email to your manager/supervisor who should then forward with their approval to our email account "invention disclosure submission." If you have any questions, please call 8-264-0444.

Last Name: McKeen	First Name: Francis (Frank)	M.I. X	
Intel Phone Number:	Intel Fax Number:	Mailstop: CO5-166	
E-mail address: frank.mckeен@intel.com		WWID: 10075788	
Citizenship: USA	Are you a contractor? Yes:	No: X	
Home Address: 10612 NW LeMans Cr.			
City: Portland	State: OR	Zip: 97229	Country: USA
Corporate Level Group: MPG	Division: MPA		Subdivision: CASA
Supervisor: Krishnan Ravichandran	WWID: 10048707	M/S: RNB6-52	Phone #: 765-5308

Last Name:	First Name:	M.I.	
Intel Phone Number:	Intel Fax Number:	Mailstop:	
E-mail address:		WWID:	
Citizenship:	Are you a contractor? Yes:	No:	
Home Address:			
City:	State:	Zip:	Country:
Corporate Level Group:	Division:		Subdivision:
Supervisor:	WWID:	M/S:	Phone #:

Last Name:	First Name:	M.I.	
Intel Phone Number:	Intel Fax Number:	Mailstop:	
E-mail address:		WWID:	
Citizenship:	Are you a contractor? Yes:	No:	
Home Address:			
City:	State:	Zip:	Country:
Corporate Level Group:	Division:		Subdivision:
Supervisor:	WWID:	M/S:	Phone #:

(PROVIDE SAME INFORMATION AS ABOVE FOR EACH ADDITIONAL INVENTOR)

2. Title of Invention: A mechanism to protect from Stack Smashing Attacks on LT

3. What technology/product/process (code name) does your invention relate to (be specific if you can) La Grande Technology

4. Include several key words to describe the technology area of the invention in addition to # 3 above:
Buffer overflow, Stack smashing, virus attack

5. Stage of development (i.e. % complete, simulations done, test chips if any, etc.): Conceptual

6a. Has a description of your invention been (or planned to be) published outside of Intel: No.

If YES, was the manuscript submitted for pre-publication approval through the Author Incentive Program:

If YES, please identify the publication and the date published:

28002

6b. Has your invention been used/sold or planned to be used/sold by Intel or others? No.

If YES, date it was sold or will be sold:

6c. Does this invention relate to technology that is or will be covered by a SIG (special interest group)/standard or specification?
No.
If YES, name of SIG/standard/specification:

6d. If the invention is embodied in a semiconductor device, actual or anticipated date of tapeout?
Could be fall of 2009

6e. If the invention is software, actual or anticipated date of any beta tests outside Intel: Soon

7. Was the invention conceived or constructed in collaboration with anyone other than an Intel blue badge employee or in performance of a project involving entities other than Intel (e.g. government, other companies, universities or consortia)? NO: If YES, name of individual or entity:

8. Is this invention related to any other invention disclosure that you have recently submitted? If so, please give the title and inventors: No.

**PLEASE READ AND FOLLOW THE DIRECTIONS ON
HOW TO WRITE A DESCRIPTION OF YOUR INVENTION**

**Try to limit your description to 2-3 pages
Do NOT attach a presentation, white paper, or specification
ANSWER ALL OF THE QUESTIONS BELOW**

Please provide a description of the invention and include the following information:

1. **Describe in detail what the components of the invention are and how the invention works.**
See folks inserted in email
2. **Describe advantage(s) of your invention over what is currently being done.**
Currently there is no defense against buffer overflows and stack smashing attacks. A proposal to support a non LT version of dual stacks has been written up in an academic paper, Architectural Support for Defending Against Buffer Overflow Attacks, Xu, Kalbarczyk, Patel, Iyer, from the Center for Reliable Computing, University of Illinois, Urbana. This proposal is not the first to propose dual stacks. In this proposal there is no need to change legacy software to support the
3. **You MUST include at least one figure illustrating the invention. If the invention relates to software, include a flowchart or pseudo-code representation of the algorithm.**
See the folioset
4. **Value of your invention to Intel (how will it be used?).**
Allows Intel computers to stop spread of virus'.
5. **Explain how your invention is novel. If the technology itself is not new, explain what makes it different.**
This invention allows virus protection of legacy code by use of the LT monitor. It allows LT to protect the LHS code integrity.
6. **Identify the closest or most pertinent prior art that you are aware of.**
See paper reference above.
7. **Who is likely to want to use this invention or infringe the patent if one is obtained and how would infringement be detected? AMD, Microsoft**

**HAVE YOUR SUPERVISOR READ AND FORWARD IT ELECTRONICALLY
VIA E-MAIL TO "INVENTION DISCLOSURE SUBMISSION"**

DATE:

SUPERVISOR:

PAGE 19/29 * RCVD AT 8/30/2007 5:35:25 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-3/11 * DNIS:2738300 * CSID:3108205988 * DURATION (mm:ss):07:40

Aug-30-07 02:33pm From-B S T Z
Rev. 10, 5/12

310 820 5988

T-161 P.020/029 F-111

BY APPROVING, I (SUPERVISOR) ACKNOWLEDGE THAT I HAVE READ AND UNDERSTAND THIS
DISCLOSURE, AND RECOMMEND THAT THE HONORARIUM BE PAID

RichEditWindow

MPG

Mobile Platforms Group

LT Stack Protection

Frank McKeen

August 28, 2007

Rev 0.1

Intel Confidential

Agenda

- Current LT value proposition
 - Solution gap
- Buffer overflow problem
- LT enhancement for stack attack mitigation

Security Concerns

MPC

Mobile Platforms Group

Activity	Risks/Concerns	Recommended Solution			
		2003	2004	2005-2006	2005-2006
Access data from enterprise	Confidential data intercepted	VPN/SSL	VPN/SSL	VPN/SSL	VPN/SSL
	Unauthorized access	PWD	TPM	TPM/LT	TPM/LT
	Display/keyboard sniffing	VPN/SSL	VPN/SSL	LT	LT
	Secure Transaction	PWD	TPM	TPM/LT	TPM/LT
E-commerce transaction	Platform authentication	VPN/SSL	VPN/SSL	VPN/SSL/LT	VPN/SSL/LT
	Secure Transaction	TRS	TRS	LT	LT
	DRM			TPM/LT	TPM/LT
	Display/keyboard sniffing	PWD	TPM	TPM/LT	TPM/LT
Email	Platform authentication	Virus scan	Virus scan	LT may help	IPSEC
	Virus protection	IPSEC	IPSEC	IPSEC	IPSEC
	Confid. email intercepted	Stack Smash	Stack Smash	Discipline	Discipline
	Use Wireless address	WEP	SSN	802.11	802.11
Notebook stolen	Wireless data security	PWD	TPM	TPM/LT	TPM/LT
	Platform authentication	PWD	Port token	Port token/LT	Port token/LT
	Data theft protection	Virus scan	Virus scan	LT may help	LT may help
	Exposed to internet	Stack Smash	Discipline	Discipline	Discipline
Use NB in public	Password stolen	Educate	Educate	Educate	Educate
	Over shoulder reading	Educate	Educate	Educate	Educate

MPC

Mobile Platforms Group

Stack Smash Attacks

- Stack Smashing attacks account for ~ 50% of security vulnerabilities reported.
- All major worms used stack smashing to bypass control of the machine
- LT does not currently solve stack smashing problem
 - LT would not protect against Code Red, Nimda, etc.
- LT impact on current internet security problems is limited to DRM and e-commerce

Enhance LT to reduce stack smashing

MPPC

Mobile Platforms Group

How Smashing works**Before attack**

Parameters
Return Address
Saved FP
Buffer[n]
Buffer
Buffer[0]
Local variable
Local variable

Stack grows downward

After attack

Parameters
Address of bypass code
Virus code
Virus code
Virus code
Virus code
Local variable
Local variable

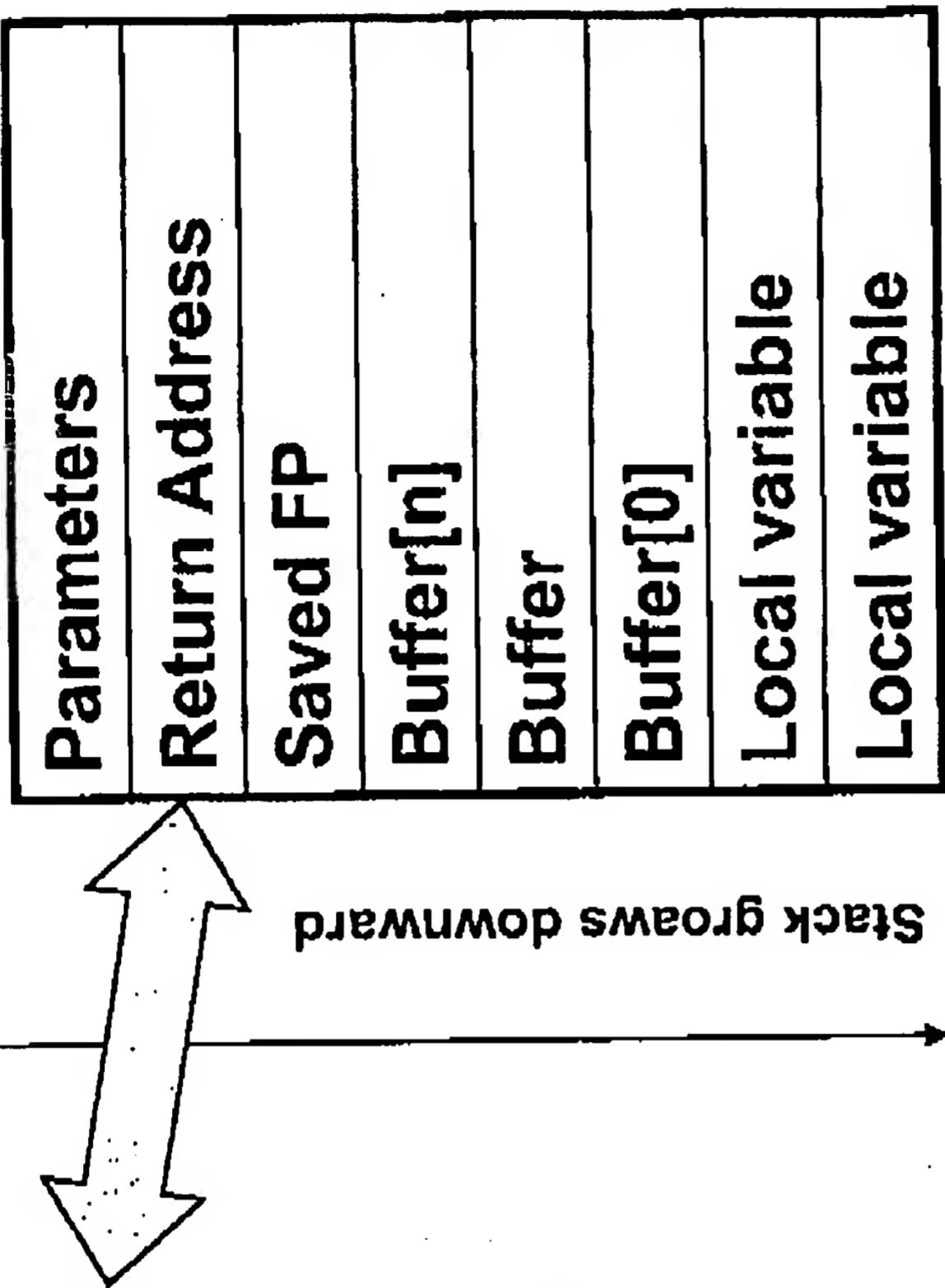
Fill buffer and more to overwrite return address

- Data is written past the end of the buffer
 - Overwrites the return address
- Return address points to code which will redirect the program to new spot

Smashing protection

New Stack

Return Address
Return Address
Return Address
Return Address

Current Stack

- Each Call deposits address in both stacks
- Each return checks that addresses match
- Failed matches are attacks.

MPCG

Mobile Platforms Group

Protection with LT

- Push the control stack into LT space where only the microcode and SVM can touch it.
 - Protects against other programs smashing both stacks
- Microcode checks two stacks to validate correct address
- VMExit generated when the two values miscompare
- VMCS contains a bit which indicates the feature is enabled for a guest
 - VMExit generated on loads to SP which relocate it.
 - Monitor maintains copy of the control stack.

Changes

- Microcode checks the values on both stacks
 - Can we experiment with patch?
- A second SP defined which points at the control stack. Each time the SP is loaded the CSP must be loaded.
- How do we determine live/dead for stacks?
 - Memory once used for stack could be kept active for a long time
 - All stacks are part of the memory image
 - Monitor keeps CSP as long as the stack is kept in memory.



Type a question for help

MPG
Mobile Platforms Group

20002-A Properties

General Summary Statistics Contents Custom

Created: Friday, March 09, 2001 1:24:51 PM
Modified: Tuesday, August 28, 2007 8:50:56 AM
Accessed: Tuesday, August 28, 2007 2:02:00 PM
Printed:

Last saved by: mycorona
Revision number: 177
Total editing time: 5409 Minutes

Statistics:	Value
Slides:	8
Paragraphs:	170
Words:	483
Bytes:	82420
Notes:	0
Hidden slides:	0
Multimedia clips:	0
Presentation format:	On-screen Show

OK Cancel

